2025

elastic security labs

RELATÓRIO GLOBAL DE PESQUISA DE AMEAÇAS

RESUMO EXECUTIVO

A era dos ataques pacientes e furtivos está dando lugar a uma nova era de ameaças de alta velocidade.

Nossa análise ano a ano revela uma mudança estratégica clara: os adversários estão se reestruturando para ganhar velocidade, utilizando a IA para gerar ameaças inéditas em larga escala e priorizando a execução imediata em vez de manter sigilo prolongado Essa aceleração força os defensores a se adaptarem a um ciclo de vida de ataque medido em minutos, não em meses, onde decisões rápidas e ricas em contexto, extraídas de dados em tempo real e históricos, tornaram-se a chave para uma defesa eficaz.

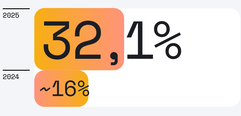
O Relatório Global de Ameaças da Elastic de 2025 do Elastic Security Labs detalha esse novo cenário.

Com base em nossa análise da telemetria de ameaças globais, identificamos os comportamentos dos adversários e as inovações defensivas que mais importam. Aqui está uma prévia do que você aprenderá:

#01

As prioridades dos adversários no Windows se inverteram

A categoria tática da **Execução** agora é responsável por **32,1%** do comportamento malicioso — dobrando sua participação anterior de ~16% — e superando a **Evasão de Defesa** como a principal tática. Isso interrompe uma tendência de três anos e indica uma mudança estratégica em direção à implantação imediata de carga útil em detrimento da furtividade inicial.



O QUE ISSO SIGNIFICA PARA VOCÊ

→ Os invasores não estão mais esperando para se esconder; eles estão focados em executar código malicioso imediatamente após a entrada. Isso torna a proteção de memória em tempo de execução e a prevenção de acesso inicial mais críticas do que nunca.

#02

A superfície de ataque na nuvem é altamente concentrada

Mais de 60% de todos os eventos de segurança na nuvem se resumem a apenas três objetivos adversários:

objetivos do adversário

/Acesso inicial
/Persistência
/Acesso às credenciais

O QUE ISSO SIGNIFICA PARA VOCÊ

→ Em todas as principais plataformas de nuvem, esse foco em **ataques baseados em identidade** é um sinal claro de que o fortalecimento dos fluxos de autenticação e o monitoramento de acessos privilegiados andmalos são as maneiras mais eficazes de defender suas cargas de trabalho na nuvem.

#03

A militarização da IA está em ascensão

Vimos um **aumento de 15,5% nas ameaças "genéricas"**, uma tendência provavelmente alimentada por adversários que usam LLMs para gerar rapidamente carregadores e ferramentas maliciosas simples, mas eficazes.

+15,5%

O QUE ISSO SIGNIFICA PARA VOCÊ

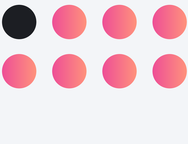
→ O aumento das ameaças geradas por IA aumenta drasticamente o volume e a variedade de malware que você enfrenta. Isso significa confiar menos em assinaturas estáticas e mais em **análises comportamentais e detecção orientada por IA** para identificar e interromper automaticamente a enxurrada de novas ameaças em redimensionar.

#04

O roubo de credenciais de navegadores é um grande negócio

>1 em 8

projetado para roubar dados do navegador



Nossa análise de mais de **150.000** amostras de malware revelou que **mais de 1 em cada 8 são projetadas para roubar dados do navegador**. Isso não é para uso isolado; essas credenciais são a matéria-prima que alimenta a **economia do broker de acesso**, fornecendo um suprimento constante de chaves para outros invasores comprometerem contas corporativas na nuvem.

O QUE ISSO SIGNIFICA PARA VOCÊ

→ O navegador é um campo de batalha primário para os dados mais sensíveis da sua organização. Os infostealers se adaptaram às proteções integradas do navegador, o que significa que os controles de identidade tradicionais não são mais suficientes.

Essas tendências estão profundamente interligadas.

Um adversário pode usar malware gerado por IA para roubar credenciais do navegador, que são então usadas para obter acesso inicial a uma conta na nuvem. Uma vez dentro, eles imediatamente se concentram na execução para implantar ransomware ou roubar dados. Este relatório conecta os pontos, mostrando como esses TTPs formam a cadeia de ataque moderna e, mais importante, como interrompê-la em vários pontos.

O cenário de ameaças é complexo, mas ao entender os comportamentos de malware e ameaças e aproveitar as defesas avançadas, as organizações podem melhorar significativamente sua resiliência.

ETAPA 1
foco na execução

ETAPA 2
obter acesso inicial a uma conta na nuvem

ETAPA 3
usar malware gerado por IA

ETAPA 4
roubar as credenciais do navegador

O Elastic Security oferece a inteligência compartilhada, os recursos avançados e os insights necessários para navegar pelas ameaças de hoje e construir um futuro mais seguro.